IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

JARED MAINES, on behalf of himself and all others similarly situated, Plaintiff, v. RECEIVABLES PERFORMANCE MANAGEMENT, LLC, Defendant.	Case No. 2:22-cv-01763 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Jared Maines ("Plaintiff") brings this Class Action Complaint against Defendant Receivables Performance Management, LLC ("RPM" or "Defendant") individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. RPM is a collections agency. RPM buys debt from banks, retailers, telecommunications companies, automobile finance companies, healthcare organizations, media companies, and others and then "provides a refreshing and intelligent alternative" to the business

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

of collecting debts from impoverished people all around the United States.[1]

2. On or about November 21, 2022, RPM reported to numerous agencies, including the Maine Attorney General, that it had been the victim of a hack that occurred between April 8, 2021 and May 13, 2021[2] (the "Data Breach"). According to RPM's disclosure to the Maine Attorney General, this hack affected 3,766,573 people.[3]

3. These individuals, rather than being customers or patients of Defendant, are people whose accounts were sent to them for collections.

4. RPM has not stated with specificity what information was contained in the hacked files, though it did note that the collections files include individuals' Social Security Numbers.[4] Social Security Numbers, used in conjunction with names and other personally indentifying information ("PII") can be very valuable in the hands of hackers.

5. Given the nature of RPM's business, there is also a reasonable chance that such files include sensitive bank, financial, or healthcare information.

6. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

7. This stolen PII has great value to hackers. Because of Defendant's Data Breach, customers' PII may be available for sale on the dark web for criminals to access and abuse. The individuals in Defendant's files face a current and ongoing lifetime risk of identity theft.

8. The information stolen in cyber-attacks allows the modern thief to assume your identity when carrying out criminal acts such as:

- Using your credit history.
- Making financial transactions on your behalf, including opening credit accounts in your name.

---

[1] http://www.receivablesperformance.com/ (last visited December 2, 2022)

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (last visited December 2, 2022)

[3] *Id.*

[4] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Stealing your smartphone's data, through a SIM-swap attack.
- Committing illegal acts which, in turn, incriminate you.

9. Plaintiff's and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class members.

10. As of this writing, there exist many class members who have no idea their PII has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

11. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of individuals for whom it had collections files, (ii) adequately warn these individuals of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates federal and state statutes.

12. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under Pennsylvania's Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. Ann. §§ 201-1 *et seq*.); and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

PARTIES

13. Plaintiff Jared Maines is a citizen of Pennsylvania, residing in Clearfield County. On or about November 23, 2022, he received notice from RPM that his PII had been involved in the Data Breach.

14. Defendant Receivables Performance Management, LLC is a Washington limited liability company with its principal place of business at 20818 44th Avenue W, Suite 240, Lynnwood, Washington. Defendant collects and maintains the personal information of millions of persons throughout the United States.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

16. This Court has personal jurisdiction over Defendant because Defendant's principal places of business are located within this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

18. RPM describes itself as "[a] national leader in Accounts Receivable Management. . .Receivables Performance Management handles accounts for retail card, credit card, health

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

insurance, auto finance, large utilities, telecommunications, and media satellite companies."[5]

19. In the normal course of business, Defendant collects PII from individuals whose collections accounts are sent to them by their clients. This PII is specifically Social Security Numbers, but when combined with names, email addresses, addresses, and phone numbers, such as those lost in the Data Breach, it gives hackers the ability to clear match Social Security Numbers to individuals. Additionally, clients may send to Defendant additional sensitive financial and health information, though the nature of that information is not currently clear.

The Data Breach

20. Defendant reported to the Maine Attorney General that the Data Breach was first discovered on or about October 2, 2022.[6]

21. In its letter to affected individuals, it states that the Data Breach occurred between April 8, 2021 and May 13, 2021, more than a year and a half ago.[7]

22. Defendant has not indicated why it took nearly a year and a half to discover that the Data Breach took place.

23. Defendant does not post a Privacy Policy, nor does it give any indication on its website that the Data Breach occurred, instead relying on direct mail to affected individuals. However, many individuals may be unaware that the Data Breach occurred, especially if they have moved residences since the time their accounts were sold to Defendant.

24. Additionally, Defendant has been vague on its response to the Data Breach, stating:

> As stated above, RPM responded immediately to the data security incident by physically disconnecting all equipment and began undertaking necessary efforts to

---

[5] https://www.linkedin.com/company/receivables-performance-management/about/ (last visited December 2, 2022)

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (last visited December 5, 2022).

[7] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1/1c35240b-8bf6-4d8e-80b4-0920997ea658/document.html (last visited December 5, 2022)

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

> restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised. Please be advised that RPM is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.[8]

25. Defendant is merely offering one year of credit monitoring with TransUnion as a result of the Data Breach. This response is entirely inadequate to Plaintiff and class members who now potentially face several years of heightened risk from the theft of their SPI and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

26. This is particularly problematic because Plaintiff's and class members' SPI was in the hands of hackers for approximately a year and a half before Defendant began notifying them of the Data Breach.

27. Defendant had obligations created by contract, industry standards, and common law to keep the PII of Plaintiff and Class members confidential and to protect it from unauthorized access and disclosure.

28. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

29. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

30. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc

---

[8] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[9] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

31. The PII of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

32. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and members of the Class, including Social Security numbers, driver license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class a result of a breach.

33. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

34. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and members of the Class.

Defendant Failed to Comply with FTC Guidelines

35. The FTC has promulgated numerous guides for businesses which highlight the

---

[9] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited December 5, 2022).

[10] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

36. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Comply with Industry Standards

40. A number of industry and national best practices have been published and should

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

41. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

The Value of PII to Cyber Criminals

42. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

43. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11]

44. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited December 5, 2022).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

> is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

45. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

46. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

47. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[14]

---

[12] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 5, 2022).

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited December 5, 2022).

[14] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 5, 2022).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

48. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

49. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

50. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

51. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

52. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

---

[15] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited December 5, 2022).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

53. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

56. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiff's and Class Members' Damages

57. To date, Defendant almost nothing to provide Plaintiff and Class members with

[16] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited December 5, 2022).

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered twelve months of identity monitoring services, which is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

58. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class members' PII.

59. Plaintiff and Class members have been damaged by the compromise of their PII in the Data Breach.

60. Plaintiff and Class members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

61. Plaintiff and Class members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegal based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class members.

62. Plaintiff and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

63. Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

64. Plaintiff and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

65. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

Data Breach

66. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

67. Further, as a result of Defendant's conduct, Plaintiff and Class members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

68. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

FACTS SPECIFIC TO PLAINTIFF

69. On or about November 25, 2022, Plaintiff was notified via a physical letter (dated November 22, 2022) from Defendant that he had been the victim of the Data Breach.

70. Plaintiff has experienced a surge in spam calls and texts roughly coincident with the timing of the Data Breach, indicating that hackers are already trying to take advantage of the release of his SPI.

71. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

CLASS ALLEGATIONS

72. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

All natural persons residing in the United States whose PII was compromised in the Data Breach announced on or about November 22, 2022 (the "Nationwide Class").

73. The Pennsylvania Subclass is defined as follows:

All natural persons residing in Pennsylvania whose PII was compromised in the Data Breach announced on or about November 22, 2022 (the "Pennsylvania Subclass").

74. The Pennsylvania Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

75. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

76. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

77. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has indicated that the PII of 3,766,573 people has been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

78. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

protection of PII belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the PII of Plaintiff and members of the Classes secure and to prevent loss or misuse of that PII;

g. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff and the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their PII had been compromised;

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief; and

k. Whether Defendant violated Pennsylvania's Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. Ann. §§ 201-1 *et seq.* (the "PUTPCPL").

79. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

80. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

81. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

82. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to each of the Statewide Subclasses as a whole.

83. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF

Negligence

(By Plaintiffs on Behalf of the Nationwide Class and the Pennsylvania Subclass)

84. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 83.

85. Defendant owed a duty to Plaintiff and the members of the Classes to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

86. The legal duties owed by Defendant to Plaintiff and the members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and members of the Classes in their possession;

b. To protect PII of Plaintiff and members of the Classes in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and members of the Classes of the Data Breach.

87. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

88. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

89. Defendant breached its duties to Plaintiff and members of the Classes. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

90. Defendant knew or should have known that their security practices did not adequately safeguard the PII of Plaintiff and the other members of the Classes.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

91. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant's unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiff and other members of the Classes during the period it was within Defendant's possession and control.

92. Defendant breached the duties they owe to Plaintiff and members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

93. Due to Defendant's conduct, Plaintiff and members of the Classes are entitled to identity theft protection. The PII taken can be used for identity theft and other types of financial fraud against the members of the Classes.

94. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

95. As a result of Defendant's negligence, Plaintiff and members of the Classes suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and members of the Classes, including ongoing credit monitoring.

96. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(By Plaintiff on Behalf of the Nationwide Class and the Pennsylvania Subclass)

97. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 83.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

99. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

100. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

101. Plaintiff and members of the Classes are within the class of persons that the FTC Act was intended to protect.

102. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Classes.

103. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current and former customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Classes.

104. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

THIRD CLAIM FOR RELIEF
Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law
73 Pa. Stat. Ann. §§ 201-1 *et seq.*
(By Plaintiff on Behalf of the Pennsylvania Subclass)

105. Plaintiff Maines re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 83.

106. Defendant has violated 73 Pa. Stat. Ann. §§ 201-1, *et seq*., by engaging in unfair or deceptive acts or practices in the conduct of trade or commerce as defined in 73 Pa. Stat. Ann. § 201-2(3) and (4) and 73 Pa. Stat. Ann. § 201-3 with respect to its conduct toward the Pennsylvania Subclass.

107. Defendant engaged in unfair or deceptive acts or practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff Maines' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff Maines' and Pennsylvania Subclass' PII in an unsecure electronic environment. Defendant also violated the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016.

108. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the data breach to the Pennsylvania Subclass members in a timely and accurate manner, contrary to the duties imposed by 73 Pa. Stat. Ann. §§ 201-1, *et seq*.

109. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Pennsylvania Subclass were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Pennsylvania Subclass' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

110. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Pennsylvania Subclass' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide Class and California Subclass.

111. Pennsylvania Subclass members seek relief under C73 Pa. Stat. Ann. §§ 201-9.2, *et seq*, including, but not limited to, restitution to Plaintiff and the Pennsylvania Subclass of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, statutory damages, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

FOURTH CLAIM FOR RELIEF
Declaratory Judgment
(By Plaintiffs on Behalf of the Nationwide Class and the Statewide Subclasses)

112. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 83.

113. Defendant owes duties of care to Plaintiff and Nationwide Class members which require it to adequately secure their PII.

114. Defendant still possess Plaintiff's and Nationwide Class members' PII.

115. Defendant has not specified what steps it has taken to prevent a data breach from occurring again.

116. Plaintiff and Nationwide Class members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

117. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Nationwide Class members for a period of ten years; and

h. Meaningfully educating Plaintiff and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(By Plaintiff on Behalf of the Nationwide Class and the Statewide Subclasses)

118. Plaintiff re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 83.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

119. Defendant benefited from receiving Plaintiff's and Nationwide Class members' PII by their ability to retain and use that information for its own benefit. Defendant understood this benefit.

120. Defendant also understood and appreciated that Plaintiff's and Nationwide Class members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

121. Plaintiff and Nationwide Class members conferred a monetary benefit upon Defendant in the form of monies paid for services from Defendant.

122. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Nationwide Class members. Defendant also benefited from the receipt of Plaintiff's and Nationwide Class members' PII, as Defendant used it to facilitate the transfer of information and payments between the parties.

123. The monies that Plaintiffs and Nationwide Class members paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

124. Defendant also understood and appreciated that Plaintiff's and Nationwide Class members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

125. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendant. Indeed, if Defendant had informed Plaintiffs and Nationwide Class members that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

126. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Nationwide Class members. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiff and Nationwide Class Members has been diminished.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

127. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff's and Nationwide Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

128. As a result of Defendant's conduct, Plaintiff and Nationwide Class members suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Nationwide Class members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

129. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Nationwide Class members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Nationwide Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

130. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Nationwide Class members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Nationwide Class members and Statewide Subclass members, request judgment against Defendant and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiff and their counsel to represent the Classes;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and the members of the Classes;

C. An order requiring Defendant to:

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

c. Audit, test, and train their security personnel regarding any new or modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiff and Nationwide Class members for a period of ten years; and

h. Meaningfully educate Plaintiff and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

D. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all members of the Classes;

E. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

F. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

G. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: December 13, 2022

Respectfully Submitted,

TURKE & STRAUSS LLP

By: */s/ Samuel J. Strauss*
Samuel J. Strauss, WSBA #46971
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com

Carl V. Malmstrom*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
malmstrom@whafh.com

Attorneys for Plaintiffs and the Class

** Pro Hac Vice Application Forthcoming*